

| NODIS Library | Legal Policies(2000s) | Search |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A

Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

[Request Notification of Change](#) (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

Chapter 20 Logical Access

20.1 Logical Access Overview

20.1.1 Logical access controls are the system-based means by which the ability to do something with an information resource is explicitly-enabled or restricted in some way. Logical access controls prescribe not only who or what, in the case of a process, is to have access to a specific system resource, but also the type of access that is permitted. Five methods of logical access control are passwords, encryption, access control lists, constrained user interfaces, and labels.

20.1.2 Logical access controls may be built into the operating system, may be incorporated into programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages. Logical access controls may be implemented internally to the IT system being protected or may be implemented in external devices.

20.1.3 External access controls are a means of controlling interactions between the system and outside people, systems, and services. External access controls use a wide variety of methods, often including a separate physical device (e.g., a computer) that is between the system being protected and a network.

20.2 Logical Access Requirements

20.2.1 NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented including, but not limited to:

- a. Implementing logical access controls on NASA systems and applications based on impact levels, policy, and permissions established by the management official responsible for the particular system, application, subordinate systems, or group of systems.
- b. Basing access control policy on the principle of least privilege.
- c. Weighing the potential impacts, costs, and benefits to the Government as a risk decision before granting any IT access.
- d. Implementing an auditable process exists for granting, establishing, and maintaining users' accounts.
- e. Ensuring that the user's identity is unique in order to support individual accountability.
- f. Considering the job assignment of the user who is seeking access to NASA IT resources in the control of access to information.

20.3 Additional Logical Access References

- a. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook.
- b. NIST SP 800-19, Mobile Agent Security.
- c. NIST SP 800-28, Guidelines on Active Content and Mobile Code.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |
[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
